DEPARTMENT OF JUSTICE SELF-INSPECTION PROGRAM DATA: FY 2015

(Submissions must be unclassified.)

Enter responses in the space below. If more space is needed, use the explanatory section at the end of this form or provide as an attachment. Contact the Security and Emergency Planning Staff, Classification Management and Policy Section with questions or for additional guidance.

PART A: Identifying Information	
1. Enter the component name.	1. Federal Bureau of Investigation
2. Enter the date of this report.	2. 09/30/2015
3. Enter the name, title, phone, fax, and e-mail address for the **point-of-contact** responsible for answering questions regarding this report.	3. [redacted] Executive Staff Unit Chief P: [redacted] / F: [redacted] [redacted]

b6
b7C

PART B: Classified National Security Information (CNSI) Program

4. Which of the following apply to your component? *(Check all that apply. If uncertain about cleared employees, request a Justice Security Tracking and Adjudication Record System (JSTARS) roster via the Personnel Security Group.)*

- ☑ Create, review, handle or store classified information
- ☐ Personnel do not process, handle or review classified information, but have a National Security Information (NSI)/ Sensitive Compartmented Information (SCI) clearance (Parts F and J of this report apply to your component)
- ☐ Office does not process, handle or review classified information and no office personnel have a NSI/SCI clearance (This report does not apply to your component)

5. Does your component contain any officials designated as an original classification authority (OCA)?	◉ Yes ○ No ○ NA
6. Does your component perform original classification activity?	◉ Yes ○ No ○ NA
7. Does your component perform derivative classification activity?	◉ Yes ○ No ○ NA

PART C: Self-Inspection Program Description

Provide a description of the component's self-inspection program to include activities assessed, program areas covered, and methodology utilized.

Activity

8. Does your component conduct self-inspection reviews? If so, who is responsible for conducting reviews? ◉ Yes ○ No ○ NA

The Chief Security Officer (CSO), or designated security personnel, is responsible for conducting security self-inspections.

9. Enter the number of self-inspections of the classified national security information program that were conducted by your component during the reporting period.	9. 1

Approach

10. What means and methods are employed in conducting self-inspections? *(For example: interviews, surveys, data calls, checklists, analysis, etc.)*

A checklist comprised of high-risk security questions is the method used to conduct security self-inspection audits. The questions are designed to accurately evaluate critical areas and to effectively assess the programs for performance/compliance risks.

Each year, half of the field offices (28 total) conduct self-inspections; therefore, each field office conducts self-inspection audits of their security program every other year. The inspection period of the self-inspection audits is from January through December of the previous year. Each field office is required to designate one point of contact to administer the self-inspection process.

It should be noted that the New York Field Office is the only office that underwent a security inspection audit in fiscal year (FY) 2015 (see explanatory comments for more information).

11. If your component performs different types of inspections (e.g., internal self-inspections, compliance reviews, etc.), describe each of them and explain how they are used. If not, indicate NA.

NA

12. Do your component's self-inspections evaluate adherence to the principles and requirements of E.O. 13526 and its implementing directive and the effectiveness of component programs covering the following areas? (*Select all that apply.*)

- ☐ Original classification
- ☑ Security violations
- ☑ Safeguarding
- ☐ Management and oversight
- ☑ Derivative classification
- ☐ Declassification
- ☑ Security education and training

13. Do your self-inspections include a review of relevant security directives and instructions?	13. ◉ Yes ○ No ○ NA
14. Do your self-inspections include interviews with producers (where applicable) and users of classified information?	14. ○ Yes ◉ No ○ NA

Approach: Representative Sample

(If your component does not classify information, indicate NA.)

15. Do your self-inspections include reviews of representative samples of original and derivative classification actions to evaluate the appropriateness of classification and the proper application of document markings?	15. ◉ Yes ○ No ○ NA
16. Do these reviews encompass all component activities that generate classified information?	16. ◉ Yes ○ No ○ NA

17. Describe below how the component identifies activities and offices whose documents are to be included in the sample of classification actions. (Indicate if NA.)

All offices produce classified information; therefore, a random selection of documents from all offices is used as a sample.

18. Do the reviews include a sampling of various types of classified information in document and electronic formats?	18. ○ Yes ◉ No ○ NA

19. How do you ensure that the materials reviewed provide a representative sample of the component's classified information? (Indicate if NA.)

The FBI reviewed classified investigative documents including but not limited to letterhead memoranda, electronic communications (ECs), Sentinel import forms, and emails. These types of documents make up the majority of classified information that the FBI produces.

20. How do you determine that the sample is proportionally sufficient to enable a credible assessment of your component's classified product? (Indicate if NA.)

In the review, patterns and trends were identified to indicate that there were specific categories of errors present in a large portion of or all of the reviewed FBI documents.

21. Who conducts the review of the classified product? (Indicate if NA.)

At the FBI, document reviews are conducted by the Executive Staff Unit (ESU), Security Division (SecD).

22. Are the personnel who conduct the reviews knowledgeable of the classification and marking requirements of E.O. 13526 and its implementing directive?	22. ◉ Yes ○ No ○ NA
23. Do they have access to pertinent security classification guides? (Indicate if NA.)	23. ◉ Yes ○ No ○ NA
24. Have appropriate personnel been designated to correct misclassification actions? If so, identify below. (Indicate if NA.)	24. ◉ Yes ○ No ○ NA

The misclassification actions can be attributed errors in the Classification Management Tool (CMT), user errors, and training gaps. Personnel have been designated to correct the errors in the CMT, disseminate awareness on common user errors, and address training gaps.

Frequency

25. How frequently are self-inspections conducted?

Each calendar year 28 field offices conduct self-inspection audits of their security program. The inspection period of the self-inspection audits is from January through December of the previous year.

26. Describe the factors that were considered in establishing this time period?

The self-inspection process was designed in order to conduct frequent self-inspections without putting undue burden on the field offices.

Coverage

27. How do you determine what offices, divisions, districts, etc., are covered by your self-inspection program? What component activities are assessed?

All field offices are covered by the FBI's self-inspection program because they all generate classified information. The self-inspection covers all activities related to derivative classification, security violations, safeguarding, and security education and training.

28. How is the self-inspection program structured to assess individual component activities and the component as a whole?

The self-inspection program assesses each field office individually. These assessments are then reviewed to determine any systemic program error(s) affecting the component as a whole.

Special Access Programs (SAPs)

29. Has your component established any SAPs within the Department and sponsored by the Attorney General?	29.	◉ Yes	○ No ○ NA
30. If so, are self-inspections of the SAPs conducted annually?	30.	○ Yes	◉ No ○ NA
31. Does your component participate in SAPs sponsored by the Intelligence Community (IC) or other government agencies?	31.	◉ Yes	○ No ○ NA
32. Does your component notify the Department Security Officer (DSO) of your participation in SAPs that are overseen by the IC or other government agencies?	32.	◉ Yes	○ No ○ NA
33. Do your component self-inspections confirm that officers and employees are aware of the prohibitions and sanctions for creating or continuing a SAP contrary to the requirements of E.O. 13526?	33.	◉ Yes	○ No ○ NA

Reporting

34. What is the format for documenting self-inspections in your component?

Each field office undergoing a self-inspection completes a checklist. The checklists are then compiled into a report

35. Who receives the reports?

SecD receives the checklists from the CSOs.

36. Who compiles/analyzes the reports?

SecD compiles and analyzes the checklists.

37. How are the findings analyzed to determine if there are problems of a systemic nature?

The findings are analyzed to identify the following:

- Field offices with low, medium, or high risk programs;
- Field offices conducting low, medium, or high quality self-inspection audit(s);
- Any systemic program error(s) in the 28 field offices, as well as the FBI Headquarters (HQ) plan of action to remedy the errors.

38. How is it determined if corrective actions are required?

Corrective actions are taken if high risk programs and low quality self-inspection audits are identified or systemic errors are found.

39. Who takes the corrective actions?

If high risk programs and low quality self-inspection audits are identified, SecD will collaborate with the corresponding field office. For any systemic program errors found, a FBI HQ plan of action is created to remedy the errors.

PART D: Declassification

40. Does your component create or maintain classified permanent records designated as such through an approved records schedule? *(If your component does not create classified permanent records this section is not applicable)*	40. ◉ Yes ○ No ○ NA
41. Does your component have an approved declassification guide and declassify CNSI?	41. ◉ Yes ○ No ○ NA

42. Describe the process and procedures for how your component accomplishes declassification reviews of your classified permanent records.

The FBI's approach to automatic declassification is to first evaluate information at the file series level. File series exemptions are sought for those file series that are national security related and the oldest information in the file series is at least 25 years old. When a file series exemption is granted, the information undergoes a review pursuant to the systematic declassification review provisions of E.O. 13526. Classified FBI information residing in non-national security related file series (or other file series that do meet the criteria for a file series exemption) is automatically declassified (without review) when the information reaches 25 years of age.

43. Do Interagency Security Classification Appeals Panel (ISCAP) approved exemptions or file-series exemptions apply to classified permanent records your component creates or maintains? If so, describe the process and procedures for how your component accomplishes systematic reviews of your exempt classified permanent records.	43. ◉ Yes ○ No ○ NA

Please see the attached document for the FBI's process and procedures.

44. Describe your component's procedures for mandatory declassification review requests received from the public.	
Please see the attached document for the FBI's process.	
45. Does your component have a process for facilitating public release or access of declassified documents, e.g., FOIA Electronic Reading Rooms, FBI Vault? If so, describe the process.	45. ◉ Yes ○ No ○ NA
Please see the attached document for the FBI's process.	
PART E: Safeguarding	
46. Is all classified material properly protected in accordance with 32 CFR Part 2001, Subpart D and the DOJ Security Program Operating Manual (SPOM), Chapter 6?	46. ◉ Yes ○ No ○ NA
47. Is all classified material transmitted in accordance with 32 CFR Part 2001, Section 2001.45 and the DOJ SPOM, Chapter 6-500?	47. ◉ Yes ○ No ○ NA
48. Is all classified material reproduction in accordance with 32 CFR Part 2001, Section 2001.44 and the DOJ SPOM, Chapter 6-402?	48. ◉ Yes ○ No ○ NA
49. Is all classified material destroyed in accordance with 32 CFR Part 2001, Section 200.46 and the DOJ SPOM, Chapter 6-600?	49. ◉ Yes ○ No ○ NA
PART F: Security Violations	
50. Is the loss, possible compromise, or unauthorized disclosure of classified information appropriately reported in accordance with the DOJ SPOM, Chapter 1-300?	50. ◉ Yes ○ No ○ NA
51. Are personnel familiar with the reporting procedures?	51. ◉ Yes ○ No ○ NA
52. What procedures are implemented to conduct an inquiry/investigation?	
In accordance with the FBI's Corporate Policy Directive 0610D, personnel who have knowledge of the loss, possible compromise or unauthorized disclosure of classified information, personally identifiable information, federal taxpayer information, or sensitive but unclassified information are required to report the circumstances to their security office. Security personnel must then notify the Security Compliance Unit (SCU), SecD, which oversees and manages the FBI's Security Incident Program. Personnel also have the option to report a security violation by filing a report in the Security Incident Reporting System (SIRS). Upon receipt, SCU ensures that all incidents are appropriately documented, investigated, and mitigated; all incidents are managed via SIRS from inception to completion. To ensure all security concerns are resolved, SCU works closely with CSOs who are charged with the responsibility to conduct an inquiry into each incident that occurs within their division.	

53. Are appropriate and prompt corrective actions taken when a security violation or infraction occurs? Describe the process.	53. ◉ Yes ○ No ○ NA

SIRS is the FBI's central database used to capture all security incidents reported by employees and personnel associated with the FBI. Upon receipt of an incident, SCU personnel work with CSOs, security professionals, or other entities as needed to ensure the incident is properly investigated and mitigated. In addition, all parties that may have a vested interest in reported security incidents are notified. For example, referrals may be made to the following entities:

- Initial Processing Unit, Inspection Division - potential misconduct
- Privacy & Civil Liberties Unit, Office Of General Counsel - potential breach of personally identifiable information
- Counterintelligence Division - potential espionage matters
- Enterprise Security Operations Center, SecD - information technology incidents
- ESU: Federal taxpayer information and information security incidents

As part of the mitigation of incidents, CSOs also conduct awareness briefings and/or provide training on security policy and procedures to individuals who commit security incidents.

54. Are individuals who commit violations or infractions subject to appropriate sanctions?	54. ◉ Yes ○ No ○ NA

PART G: Management and Oversight

55. How many personnel are dedicated to manage the classified national security information program?	55. 3
56. Are sufficient resources and personnel committed to implement the classified national security information program? If no, please explain.	56. ○ Yes ◉ No ○ NA

More dedicated personnel are required to provide more customized support across the FBI. Three employees can not adequately support the needs of almost 48,000 personnel. For example, in FY 2015, 12 requests for customized, in-person training were received that ESU could not fulfill due to decreased personnel and heavy workload.

PART H: A summary of the findings of your component's self-inspection program
(If portions are not applicable to your component, indicate NA.)

The **summary** should present specific, concise findings from your self-inspection program for each of the required program areas below. It is not a description of the requirements of the component's CNSI program. Rather, the summary outlines the essential self-inspection findings based on the compilation and/or distillation of the information contained in the component's internal self-inspection reports, checklists, etc.

57. Original Classification:

NA

58. Derivative Classification:

A classified information training program is maintained that provides initial briefings and refresher training. Personnel are aware of the process and requirements for derivative classification.

59. Declassification:

NA

60. Safeguarding:

Control measures to prevent unauthorized access to classified information are implemented. Classified information is handled, stored, and transmitted in a way that prevents loss or compromise. A system of security checks to ensure that classified information is properly secured happens periodically as opposed to the end of every day. Security awareness briefings are conducted twice annually to provide information on proper safeguarding procedures.

61. Security Violations:

All personnel are aware of the procedure for reporting security violations. Appropriate actions are taken when a violation or infraction occurs. Individuals who commit violations or infractions are subject to appropriate sanctions.

62. Security Education and Training:

A classified information training program is maintained that provides initial briefings, refresher training, and termination briefings. Records are kept of all trainings and briefings provided. Security awareness briefings are conducted twice annually to provide information on proper security practices. Posters with security tips are distributed throughout the offices. Several security courses are currently being developed for personnel.

63. Management and Oversight:

NA

PART I: An assessment of the findings of your component's self-inspection program
(If portions are not applicable to your component, indicate NA.)

The **assessment** discerns what the findings mean. The assessment is an evaluation of the state of each element of your component's CNSI program based on an analysis of the specific, concise findings of the self-inspection program. It reports what you have determined the findings indicate about the state of your component's CNSI program.

The assessment should inform the DSO and other decision makers of significant issues that impact the CNSI program. It should be used to determine how security programs can be improved, whether the agency regulation or other policies and procedures must be updated, and if necessary resources are committed to the effective implementation of the CNSI program. The assessment should report trends that were identified during the reporting period across the component or in particular activities, as well as trends detected by making comparisons with earlier reporting periods. It can be used to support assertions about the successes and strengths of a component's program.

64. Original Classification:

NA

65. Derivative Classification:

Based on the findings, the FBI is able to successfully derivatively classify information.

66. Declassification:

NA

67. Safeguarding:

Based on the findings, the FBI has a well rounded security program to protect FBI information and information systems through training and awareness to prevent malicious use, compromise, or unauthorized disclosure of classified information.

68. Security Violations:

Based on the findings, the FBI has a comprehensive security incident program that allows for incidents to be easily reported and corrective actions taken.

69. Security Education and Training:

Based on the findings, the FBI has a robust training program for information security. Vulnerabilities are addressed through a multifaceted training and awareness approach.

70. Management and Oversight:

NA

PART J: Focus Questions

Answer the questions below. If the response identifies a deficiency, it should be explained in Part D, Summary of Findings, under the relevant program area, and should be addressed in Part H, Corrective Actions.

Training for Original Classification Authorities

Original classification authorities are required to receive training in proper classification and declassification each calendar year. (Section 1.3(d) of E.O. 13526 and § 2001.70(c) of 32 C.F.R. Part 2001) (Indicate NA if your component does not have original classification authority.)

71. How many original classification authorities exist within the component?	71. 17
72. What percentage of the original classification authorities at your component has received annual training?	72. 100 ◉ Actual ○ Estimated
73. Have any waivers to this requirement been granted?	73. ○ Yes ◉ No ○ NA

Persons who Apply Derivative Classification Markings

Persons who apply derivative classification markings are required to receive training in the proper application of the derivative classification principles of E.O. 13526, prior to derivatively classifying information and at least once every two years thereafter. (Section 2.1(d) of E.O. 13526 and § 2001.70(d) of 32 C.F.R. Part 2001) (Indicate NA if your component does not have any personnel who derivatively classify information.)

74. How many derivative classifiers exist within the component?	74. 47,950
75. What percentage of the derivative classifiers at your component received training prior to derivatively classifying information?	75. 100 ◉ Actual ○ Estimated
76. What percentage of the derivative classifiers at your component has received refresher training?	76. 96 ○ Actual ◉ Estimated
77. Have any waivers to this requirement been granted?	77. ○ Yes ◉ No ○ NA

Initial Training

All cleared component personnel are required to receive initial training on basic security policies, principles, practices, and criminal, civil, and administrative penalties. (§ 2001.70(b) of 32 C.F.R. Part 2001)

78. How many cleared federal and contract employees exist within the component?	78. 47,950
79. What percentage of cleared employees at your component has received initial training?	79. 100 ◉ Actual ○ Estimated

Annual Refresher Training

Agencies are required to provide annual refresher training to all employees who create, process, or handle classified information. (§ 2001.70(f) of 32 C.F.R. Part 2001)

80. What percentage of the cleared employees at your component has received refresher training?	80. 96 ○ Actual ◉ Estimated

Identification of Derivative Classifiers on Derivatively Classified Documents

Derivative classifiers must be identified by name and position, or by personal identifier on each classified document. (Section 2.1(b)(1) of E.O. 13526 and § 2001.22(b) of 32 C.F.R. Part 2001) (Indicate NA if your component does not derivatively classify information.)

81. Does your component's review of classification actions evaluate if this requirement is being met?	81. ◉ Yes ○ No ○ NA
82. What percentage of the documents sampled meet this requirement?	82. 22
83. What was the number of documents reviewed for this requirement?	83. 510

List of Sources on Documents Derivatively Classified from Multiple Sources

A list of sources must be included on or attached to each derivatively classified document that is classified based on more than one source document or classification guide. (§ 2001.22c(1)(ii) of 32 C.F.R. Part 2001)

84. Does your component's review of classification actions evaluate if this requirement is being met?	84. ◉ Yes ○ No ○ NA
85. What percentage of the documents sampled meet this requirement?	85. 95
86. What was the number of documents reviewed for this requirement?	86. 510

Performance Evaluations

The performance contract or other rating system of original classification authorities, security managers, and other personnel whose duties significantly involve the creation or handling of classified information must include a critical element to be evaluated relating to designation and management of classified information. (Section 5.4(d)(7) of E.O. 13526) ("Significantly" is defined as an individual who has access to a classified network.)

87. How many personnel within your component perform duties that significantly involve the creation or handling of classified information as defined above?	87. 47,950
88. What percentage of such personnel at your component has this critical element in their performance evaluations?	88. 100 ◉ Actual ○ Estimated

OCA Delegations	
OCA delegations shall be reported or made available by name or position to the Director of the Information Security Oversight Office. (Section 1.3(c)(5) of E.O. 13526). This can be accomplished by an initial submission followed by updates on a frequency determined by the SAO, but at least annually. (§2001.11(c) and §2001.90(a) of 32 C.F.R. Part 2001)	
89. Have all delegations been limited to the minimum required based on a demonstrable and continuing need to exercise this authority?	89. ◉ Yes ○ No ○ NA
Industrial Security	
The National Industrial Security Program (NISP) was established under E.O. 12829 to safeguard Federal Government classified information that is released to contractors, licensees, and grantees (hereinafter contractors) of the United States Government. Under the NISP, contractors are mandated to protect all classified information to which they have been given access or custody by U.S. Government Executive Branch Department or Agencies.	
90. Does your component have contracts that require access to classified national security information (CNSI), hereinafter referred to as classified contracts?	90. ◉ Yes ○ No ○ NA
91. If your component issues classified contracts, does it provide the contractor with current security classification guidance?	91. ◉ Yes ○ No ○ NA
92. Are the contractor's security requirements issued through either a specific contract clause or by a Contract Security Classification Specification (DD-254)?	92. ◉ Yes ○ No ○ NA

PART K: Findings of the Annual Review of Component's Original and Derivative Classification Actions		
In this section provide specific information with regard to the findings of the annual review of the component's original and derivative classification actions to include the volume of classified materials reviewed and the number and type of discrepancies identified.		
93. Indicate the volume of classified materials reviewed during the annual review of original and derivative classification actions. (If your component does not classify information, indicate NA.)	93.	510
94. Indicate the number of discrepancies found during the annual review of classification actions for each category below. For additional information on marking, consult the DOJ marking guide and ISOO marking guide.		
(a) Over-classification: Information does not meet the standards for classification.	(a)	0
(b) Overgraded/Undergraded: Information classified at a higher/lower level than appropriate.	(b)	0
(c) Declassification: Improper or incomplete declassification instructions or no declassification instructions.	(c)	0
(d) Duration: A shorter duration of classification would be appropriate.	(d)	0
(e) Unauthorized classifier: A classification action was taken by someone not authorized to do so	(e)	0
(f) "Classified By" line: A document does not identify the OCA or derivative classifier by name and position or by personal identifier.	(f)	399
(g) "Reason" line: An originally classified document does not cite a reason from section 1.4 of E.O. 13526.	(g)	0
(h) "Derived From" line: A document fails to cite, or cites improperly, the classification source. The line should include type of document, date of document, subject, and office/component of origin.	(h)	0
(i) Multiple sources: A document cites "Multiple Sources" as the basis for classification, but a list of these sources is not included on or attached to the document.	(i)	23
(j) Marking: A document lacks overall classification markings or has improper overall classification markings.	(j)	16
(k) Portion Marking: The document lacks some or all of the required portion markings	(k)	278
(l) Instructions from a classification guide are not properly applied.	(l)	0
(m) Other (*specify*):	(m)	

PART L: Corrective Actions

95. Describe actions that have been taken or are planned to correct identified program deficiencies, marking discrepancies, or misclassification actions, and to deter their reoccurrence.

The primary cause of the referenced discrepancies falls into two categories:

CMT – The CMT is deployed on several FBI platforms, including Microsoft Applications (e.g., Outlook) and Sentinel. Currently, there are inconsistencies among versions of the CMT since there are multiple versions of the CMT running across the enterprise. SecD is working with Information Technology Engineering Division to ensure the same updated version of the CMT is deployed throughout the FBI.

User Errors – To reduce and mitigate errors, the FBI continued to provide training awareness on correct classification marking and handling procedures to all FBI personnel. The FBI is developing a new user friendly web-based training for designating, marking, and handling classified information. Security bulletins will be disseminated to notify FBI personnel of newly-available resources, such as the publication of a new classification guide, or to provide awareness of common marking errors in order to correct problematic trends.

PART M: Best Practices

Best practices are those actions or activities that make your self-inspection program and/or CNSI program more effective or efficient. They set your program apart through innovation or by exceeding the minimum program requirements. These are practices that may be utilized or emulated by other agencies.

96. Describe best practices that were identified during the self-inspection.

The FBI uses a multi-layered approach of training awareness to address information security trends and identification of errors through both incident reporting and annual document reviews. In addition to the required annual Information Security (INFOSEC) Course, the FBI is developing a new user friendly web-based training for designating, marking, and handling classified information, which will be mandatory for all users of FBI systems.

The FBI is currently using the CMT to mark classified information. Over 22 FBI information technology systems are using a marking tool to mark classified information. The CMT correctly formats a banner line and portion marks on classified documents. It is the goal of the FBI to have all FBI systems using the same version of the CMT to ensure current marking standards and rules are applied.

PART N: Explanatory Comments

97. Use this space to elaborate on any section of this form. If more space is needed, provide as an attachment to this form. Provide explanations for any significant changes in trends/numbers from the previous year's report.

For FY 2015, the only self-inspection conducted was at the New York Field Office at their request. No other self-inspections were conducted as Security Division has been restructuring and developing a new self-inspection process to be implemented for FY 2016. Part H and Part I are findings and assessments related solely to the New York Field Office.

Question 30: The SAP was just recently established so a self-inspection has not been conducted. Self-inspections will be conducted annually in the future.

Submit